Amendments to the Specification:

Please replace the paragraph beginning on Page 8, line 6, with the following amended paragraph:

In a further embodiment, the outputs t_j of the cipher functions f ($t_j = f(m_j, k_j)$, for j = 0 to 7) and the outputs of the inverse cipher function f^{-1} ($t_j = f^{-1}(m_j, k_j)$, for j = 8 to 15) are swapped in the following manner: t_j <-> t_{15-j} for j = 0 to 7 and the swapped sub-blocks are concatenated to form a single result. This is illustrated in Figure 7.